CHAPTER 7

CYBERCRIME IN 2011

Jason Gonzalez, Matthew A. S. Esworthy, and Eric Nemecek

I. INTRODUCTION

Cybercrime law continued to evolve in 2011 as it struggled to keep up with changes in technology and the way people use it. The past year saw the rise of international organized hacking groups, major corporate hacking and data breach scandals, and efforts by law enforcement to improve its tactics to remain effective. Courts and legislatures similarly struggled with applying the law to situations never contemplated just a few years ago. And the cybercrime problem seems only to be getting worse, with 2011 seeing a 37.4% increase in the number of reported hacking incidents, and a survey of 4,000 international business leaders finding that cybercrime is one of the top four economic crimes they face.[1]

II. THE RISE OF ORGANIZED HACKING GROUPS

Perhaps the most notable cybercrime trend in 2011 was the rise of "organized" hacking groups such as Anonymous and LulzSec. Such groups claim a quasi-political or social agenda that goes beyond the desultory pranks often associated with hacking. Many of their attacks reflected such claimed agendas, including alleged denial of service attacks on financial institutions perceived to have wronged the "wikileaks" website operators, attacks to shut down or deface the websites of repressive Arab governments, and hacks of Sony Corporation in claimed retaliation for Sony's legal action against a software developer.

The groups' organization, agendas, and high public profile made them of significant concern to law enforcement. As with many Internet-based cybercrimes, however, investigation and prosecution of such groups can be challenging. Membership is fluid and informal, and the group "members" are often difficult to identify as they typically use online nicknames and techniques to make themselves difficult to electronically trace. Moreover, the members, and the evidence associated with their conduct, can be scattered around the world, requiring investigators to deal with sometimes complicated issues of jurisdiction and international cooperation. Law enforcement nonetheless has issued dozens of search warrants related to these groups' attacks, and made a number of arrests in the United States and overseas.[2]

III. CORPORATE HACKING

The News of the World phone-hacking scandal brought sustained public attention to a type of cybercrime that perhaps may only get more common – corporate-sponsored hacking. While there have been many examples of corporate, and even state-sponsored, hacking in past years, the News of the World scandal seemed particularly captivating, perhaps because it involved apparent corporate-sponsored hacking of the personal telephone voicemails of private individuals. Done in an apparent effort to generate news stories, the scheme involved reporters hacking into the voicemails of the family of a murdered schoolgirl, soldiers returning from war, and victims of terror attacks, as well as the British royal family and other celebrities. While consequences for the News of the World were severe – including going out of business, public

outrage directed at executives, and ongoing criminal investigations – the general deterrence value of such consequences is questionable. As mobile devices and cloud computing enable individuals to store increasing amounts of highly personal and sensitive data electronically, this sensitive data, on a theoretical level at least, becomes susceptible to hacking and exposure. This provides a tempting target for cybercriminals, including cybercriminals working at organizations for which such personal data may have business value.

IV. THE GOVERNMENT

The government's activity in the past year included notable efforts to address cybercrime in innovative ways. One example is the government's increased use of its power to seize Internet domain names associated with criminal activity. On November 28, 2011, the Department of Homeland Security announced that it had seized 150 website domains associated with counterfeit and pirated goods as part of DHS's "Operation In Our Sites" program. In this program, undercover federal agents made online purchases of suspected counterfeit or pirated merchandise and, after confirmation with the true owner that the merchandise was illegal, obtained court orders permitting the government to seize the offending website. Since the operation was launched in June 2010, the DHS has seized a total of 350 domain names.[3]

Another example of the government's efforts to innovate is its forging of collaborations to address the often multi-jurisdictional and international nature of cybercrime. In November 2011, for example, the government announced that US federal, Estonian, and Dutch law enforcement worked together to secure the arrest of six Estonian nationals who will be prosecuted in the US for running an Internet fraud ring that affected millions of users worldwide. The government collaborated with the US private sector in taking down the "Coreflood" botnet in 2011, including working with anti-virus and software companies to detect and remove the virus from infected computers. The US government also worked closely with the Chinese government to investigate and prosecute a US citizen that allegedly was running eighteen Chinese-language child pornography websites targeting customers in China and elsewhere.[4]

Lastly, the US government underscored the increasing seriousness of the cybercrime threat to national security when a Pentagon spokesman made statements indicating that, depending on the circumstances, cyberattacks could be considered an act of war that would justify retaliation with conventional weapons.[5]

V. THE COURTS

The courts faced particularly difficult challenges applying traditional legal principles to new technology. The Supreme Court wrestled with applying the Fourth Amendment to global positioning system ("GPS") technology when it heard oral argument in early November 2011 in *United States v. Jones*, which concerned the propriety of law enforcement surveillance using a GPS device. In *Jones*, law enforcement officers, acting without a warrant, attached a GPS device to the defendant's car and thereby tracked his movements continuously for a month.[6] The prosecution alleged that this GPS data showed the defendant's participation in a narcotics conspiracy, but the defendant moved to suppress, claiming the use of the GPS device amounted to an impermissible Fourth Amendment search.[7] The D.C. Circuit reversed the district court's denial of the motion, finding that the application of the GPS device amounted to an impermissible search, and noting that "the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave."[8] The D.C. Circuit distinguished the use of the GPS device in *Jones* from the use of a "beeper" tracking device

approved of in *United States v. Knotts*,[9] noting that *Knotts* dealt with tracking a suspect's movements for only one relatively short trip, not the extended "twenty-four hour surveillance" the GPS device enabled.[10]

On January 23, 2012, the Supreme Court found that the installation of a GPS monitoring device constituted a warrantless search subject to suppression under the Fourth Amendment. Justice Scalia's Opinion for the Court noted that it "is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[11] The Majority undertook a lengthy discussion of the evolution of the Court's Fourth Amendment jurisprudence concerning whether a "search" has occurred.[12] In support of its conclusion that installation of the GPS device constituted a "search" in this instance, the Court first determined that the act of installing the device was a physical intrusion (i.e. "trespass") for the purpose of obtaining information. In so holding, the Court departed from the analysis that was applied in *Katz v. United States*,[13] which focused solely on whether the defendant exhibited and maintained a reasonable expectation of privacy in the area searched by the Government. The Court explained that its previous holding in *Katz* was not intended to limit the protections afforded by the Fourth Amendment; rather the Court reasoned that "the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test."

Perhaps the most interesting aspect of the *Jones* decision is the uncertainty that it has created. While the Government's physical intrusion was a cornerstone of the Majority's reasoning, the Court did not imply that its decision would have been different had there not been an initial trespass: "our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[14] The Court declined to consider whether the installation of GPS is a search that *requires* a warrant, although at least four members of the Court suggested that long-term monitoring of a GPS device would necessitate a warrant. Justice Alito's concurrence (joined by Justices Ginsburg, Breyer and Kagan), argued that the Court should apply a more *Katz*-oriented analysis in considering whether GPS monitoring intrudes on an expectation of privacy that society recognizes as reasonable: "[u]nder this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[15] Justice Alito also opined that courts should consider the nature of the offense being investigated in determining the reasonableness of the Government conduct: "[b]ut the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." The Court's reluctance to "grapple with these 'vexing problems'" highlights the continued challenges we face by applying a document drafted in 1789 – when mail could take months to travel across the Atlantic – to today's technology – when data can span the globe in a matter of seconds.[16]

Another highly controversial case from 2011 is *United States v. Nosal*,[17] in which the Ninth Circuit ruled that a criminal violation of the Computer Fraud and Abuse Act can be based on an employee's violation of his employer's computer access restrictions. The defendant in *Nosal* worked with co-conspirators to obtain information from his employer's computer system to set up a competing business.[18] The employer's computer system had a warning message that appeared during the log-in process which indicated that the system and its data were the employer's property and that misuse of it could lead to criminal prosecution.[19] The defendant

was charged with violating Section 1030(a)(4) of the CFAA, which subjects to punishment anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value."[20] The Ninth Circuit held that, by knowingly violating his company's computer access restrictions, the defendant "exceeded authorized access" under the CFAA, and therefore was subject to prosecution.[21] The dissent, and many commentators, pointed out that reading the phrase "exceeds authorized access" as equivalent to knowingly violating an employer's computer access restrictions would criminalize the conduct of millions of people who, during the course of their work, use their employer-issued computer to occasionally check personal email or sports scores online.[22] The majority opinion also, according to its critics, would make the CFAA unconstitutionally vague, in that criminal liability would be premised on the employers' wording of their access restrictions, which "are not necessarily drafted with the definiteness or precision that would be required for a criminal statute."[23] In October 2011, the Ninth Circuit agreed to rehear the case *en banc*, and heard oral argument in mid-December 2011.

The California Supreme Court created headlines when it decided *People v. Diaz*.[24] In *Diaz*, the court held that law enforcement could lawfully search, without a warrant, a cell phone seized from a suspect incident to the suspect's arrest. In its analysis, the court relied upon US Supreme Court precedent approving searches incident to arrest of suspects' clothing and items found in shirt pockets, including *United States v. Edwards*,[25] and *United States v. Robinson*.[26] The dissent, as well as commentators, noted that cell phones can potentially contain vast quantities of highly personal data, and thus are qualitatively different and therefore should not be subject to the same analysis: "The United States Supreme Court's holdings on clothing and small spatial containers were not made with mobile phones, smartphones and handheld computers – none of which existed at the time – in mind."[27] After this controversial decision, the California legislature passed a bill which would have nullified the *People v. Diaz* ruling and have required that portable electronic devices could not be searched incident to arrest absent a search warrant. In October 2011, however, California Governor Jerry Brown vetoed the bill, meaning that *People v. Diaz* still applies in California.

Other noteworthy cases from 2011 include *Griffin v. State of Maryland*,[28] in which the court discussed techniques to overcome the challenges in authenticating evidence from social networking sites, including (most obviously) eliciting testimony from the alleged creator of the social networking evidence, performing a forensic analysis of the computer associated with the site's user, and subpoenaing or otherwise obtaining information from the social networking site provider that may associate a particular user with the social networking evidence at issue.[29] In *Glik v. Cunniffe*,[30] the First Circuit confirmed that the First Amendment protects the rights of citizens to openly video record police officers engaged in their duties. The court noted: "[t]he proliferation of electronic devices with video-recording capability means that many of our images of current events come from bystanders with a ready cell phone or digital camera rather than a traditional film crew. . . . Such developments make clear why the news-gathering protections of the First Amendment cannot turn on professional credentials or status."[31] Lastly, in *United States v. Cotterman*,[32] the Ninth Circuit held that a law enforcement search of a computer seized at the US border was a proper "border search," despite the fact that the search itself occurred nearly 170 miles away at a forensic laboratory. As the Ninth Circuit put it, "the border search doctrine is not so rigid as to require the United States to equip every entry point – no matter how desolate or infrequently traveled – with inspectors and sophisticated forensic equipment . . . or be otherwise precluded from exercising its right to protect our nation absent some heightened suspicion."[33]

VI. LEGISLATIVE EFFORTS

The most significant cyber crime related legislative activity concerned proposed amendments to the Computer Fraud and Abuse Act ("CFAA"). The CFAA was passed in 1986 and originally was motivated by a desire to penalize traditional "hacking" activities. It has been amended several times since, and was subject in 2011 to efforts to amend it further. Some sought to increase its scope and the punishment it imposes; others contended it is overbroad and should be limited.

The US Department of Justice is among those seeking to increase the CFAA's scope and authorized punishments. These changes are necessary, according to the DOJ, because the volume, severity, and sophistication of cyber crime is growing, and because cybercrime is difficult to prosecute under current laws, particularly in that the Internet allows the perpetrators to be relatively anonymous and reside anywhere in the world. The DOJ also contends that, while in the past computer crime primarily was motivated by curiosity, more recently hacking has become motivated by financial gain and has become a tool of organized criminal gangs. There is also increased concern that hacking could affect national critical infrastructure, including the power grid and water supply.[34]

The DOJ proposed amendments to the CFAA that seek to address these concerns. They include amendments that would: (1) make computer crimes a "predicate offense" under the Racketeer-Influenced Corrupt Organizations Act; (2) increase the statutory maximum penalties; (3) amend the language regarding the offense of trafficking in passwords to ensure that it is clear that it covers crimes related to all authentication mechanisms; (4) add a civil forfeiture provision; and (5) impose a three-year mandatory minimum sentence for crimes involving a compromise of "critical infrastructure."[35]

Others have criticized the CFAA as being overbroad. These critics have focused their attention on the fact that the CFAA, as written, has been interpreted to allow criminal prosecutions based on violations of "terms of service" imposed by Internet service providers, websites, and others, as well as prosecutions similarly based on a violation of an employer's "acceptable use" policies (as in *Nosal*, discussed above). Such prosecutions, the critics claim, go well beyond the original intentions of the CFAA and, more importantly, criminalize vast amounts of fairly innocent, common behavior, such as using an alternate identity while online. They have proposed refinement of definitions in the CFAA to clarify that a person does not "exceed authorized access" by merely violating a terms of service or "acceptable use policy." There is also some concern that essentially any computer-related crime will amount to a federal crime prosecutable under the CFAA, as the term "protected computer" can easily be read to cover every computer connected to the Internet.

Another highly controversial legislative development is the promulgation of anti-piracy bills, including the Stop Online Piracy Act and the Protect Intellectual Property Act. These bills generally give intellectual property rights holders the ability to seek court orders against websites that facilitate copyright infringement. These orders can result in the websites being rendered inaccessible, and any payment or advertising services being ordered to cease working with the offending websites. The bills have been supported by the Motion Picture Association of America, the Recording Industry of America, publishers, and other "rights holders." Many in the technology industry have opposed the bills, including Google, eBay, Yahoo, Facebook, AOL, Twitter, and Zynga. Those opposed to these bills have contended that the bills will seriously compromise the security of the Internet, will set a dangerous precedent that will encourage other countries to similarly "blacklist" certain websites, and will not ultimately limit copyright

infringement over the Internet in that the technical restrictions imposed on the offending sites can easily be circumvented. In early 2012, in the face of fierce opposition, the major sponsors of these bills rescinded their support and the legislation, at least for the time being, appears to have been stalled.

VII. CONCLUSION

The past year saw cybercrime increase in volume and sophistication, and efforts by law enforcement, the courts, and the legislature to combat it strive to keep up. What will 2012 bring? In such a rapidly-evolving field, it is difficult to say. We can be sure, however, that the struggle between innovative technology and the deliberative pace of the law will continue to manifest itself in fascinating ways.

Endnotes, Chapter 7

[1] Bloomberg Business Week Year in Review, "Data Security: Your Information, Their Loot," (December 26, 2011 – January 8, 2012); PricewaterhouseCoopers, "Cybercrime: protecting against the growing threat," Global Economic Crime Survey (November 2011).

[2] "FBI Arrests U.S. Suspect in LulzSec Sony Hack; Anonymous Also Targeted," Wired.com (September 22, 2011).

[3] U.S. Immigration and Customs Enforcement press release, "Operation In Our Sites protects American online shippers, cracks down on counterfeiters" (November 11, 2011).

[4] Federal Bureau of Investigation press release, "Operation Ghost Click" (November 9, 2011); Federal Bureau of Investigation press release, "Botnet Operation Disabled" (April 14, 2011); Federal Bureau of Investigation press release, "18 Child Porn Websites Shut Down" (October 11, 2011).

[5] *See* "US Pentagon to treat cyber-attacks as 'acts of war,'" BBC News (June 1, 2011).

[6] United States v. Jones, 615 F.3d 544, 549 (D.C. Cir. 2010).

[7] *Id.* at 556, 568.

[8] *Id.* at 565.

[9] 460 U.S. 276 (1983).

[10] *Id.* at 556.

[11] *Jones,* 2012 WL 171117 (Jan.23, 2012) at *3.

[12] *Id.*

[13] 389 U.S. 347 (1967).

[14] *Jones*, 2012 WL at *7.

[15] *Id*. at *17.

[16] *Id*. at *7.

[17] 642 F.3d 781 (9th Cir. 2011).

[18] *Id*. at 782.

[19] *Id*. at 784.

[20] 18 U.S.C. § 1030(a)(4).

[21] *Id.* at 788.

[22] *Id.* at 789-90.

[23] *Id*. at 790.

[24] 51 Cal.4th 84 (2011).

[25] 415 U.S. 800 (1974).

[26] 414 U.S. 218 (1973).

[27] *Id.* at 516-17.

[28] 19 A.3d 415 (2011).

[29] *Id*. at 427-48.

[30] 655 F.3d 78 (1st Cir. 2011).

[31] *Id.* at 84.

[32] 637 F.3d 1068 (9th Cir. 2011).

[33] *Id.* at 1070.

[34] Statement of Richard W. Downing, Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, Before the House Committee on Judiciary Subcommittee on Crime, Terrorism, and National Security, presented November 15, 2011.

[35] *Id*.